


STANDARD OPERATING PROCEDURE (SOP)		Section 8
DETROIT POLICE DEPARTMENT		
Crime Intelligence Unit		
	EFFECTIVE DATE 7/1/2018	REVISED DATE 4/1/2019
	TOTAL SECTION PAGES: 9	
	SUBJECT 8. FACIAL RECOGNITION	
APPROVED BY: Deputy Chief Marlon Wilson		

8.1. DEFINITIONS

- (a) *Biometric data* – Data derived from one or more intrinsic physical or behavioral traits of humans, to include fingerprints, palm prints, iris scans, and facial recognition data.
- (b) *DataWorks Plus* – The company with which DPD has a contract to provide facial recognition software.
- (c) *Facial recognition (FR)* – The automated searching of a facial image in a biometric database (one-to-many), typically resulting in a group of facial images ranked by computer-evaluated similarity.
- (d) *Examiner* – An individual who has received advanced training in the face recognition system and its features. Examiners have at least a working knowledge of the limitations of face recognition and the ability to use image editing software. They are qualified to assess image quality and appropriateness for face recognition searches and to perform one-to-many and one-to-one face image comparisons.
- (e) *Highly Restricted Personal Information* – An individual's photograph or image, social security number, digitized signature, medical and disability information.
- (f) *Mobile Facial Recognition (Mobile FR)* – The process of conducting an automated FR search in a mobile environment.
- (g) *P/CRCL* – Privacy, civil rights, and civil liberties.
- (h) *Personally Identifiable Information (PII)* – Information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.
- (i) *Statewide Network of Agency Photos (SNAP)* – A computer application managed by the SNAP Unit, deployed through the Michigan Criminal Justice Information Network (MiCJIN) Portal, which serves as an investigative tool and a central repository of images from local, state, and federal agencies.

8.2. PURPOSE

- (a) Facial recognition technology involves the ability to examine and compare distinguishing characteristics of a human face through the use of biometric algorithms contained within a

software application. This technology can be a valuable investigative tool to detect and prevent criminal activity, reduce an imminent threat to health or safety, and help in the identification of persons unable to identify themselves or deceased persons. DPD has established access and use of a face recognition system to support its investigative efforts.

- (b) It is the purpose of this policy to provide CIU personnel with guidelines and principles for the collection, access, use, dissemination, retention, and purging of images and related information applicable to the implementation of a face recognition (FR) program. This policy will ensure that all FR uses are consistent with authorized purposes while not violating the privacy, civil rights, and civil liberties (P/CRCL) of individuals. Further, this policy will delineate the manner in which requests for face recognition are received, processed, catalogued, and responded to. The Fair Information Practice Principles (FIPPs) form the core of the privacy framework for this policy. This policy assists the CIU and its personnel in:
 - i. Increasing public safety and improving state, local, tribal, territorial, and national security.
 - ii. Minimizing the threat and risk of injury to specific individuals.
 - iii. Minimizing the threat and risk of physical injury or financial liability to law enforcement and others responsible for public protection, safety, or health.
 - iv. Minimizing the potential risks to individual privacy, civil rights, civil liberties, and other legally protected interests.
 - v. Protecting the integrity of criminal investigatory, criminal intelligence, and justice system processes and information.
 - vi. Minimizing the threat and risk of damage to real or personal property.
 - vii. Fostering trust in the government by strengthening transparency, oversight, and accountability.
 - viii. Making the most effective use of public resources allocated to public safety entities.
- (c) All deployments of the face recognition system are for official use only/law enforcement sensitive (FOUO/LES). The provisions of this policy are provided to support the following authorized uses of face recognition information:
 - i. A reasonable suspicion that an identifiable individual has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal conduct or activity.
 - ii. An active or ongoing criminal or homeland security investigation.
 - iii. To mitigate an imminent threat to health or safety through short-term situational awareness or other means.
 - iv. To assist in the identification of a person who lacks capacity or is otherwise unable to identify him- or herself (such as an incapacitated, deceased, or otherwise at-risk person).
 - v. To investigate and/or corroborate tips and leads.
 - vi. For comparison to determine whether an individual may have obtained one or more official state driver's licenses or identification cards that contain inaccurate, conflicting, or false information.

- vii. To assist in the identification of potential witnesses and/or victims of violent crime.
 - viii. To support law enforcement in critical incident responses.
- (d) In the event that DPD deploys a mobile FR, mobile face image searches may be performed only by a sworn officer who has completed training and only during the course of an officer's lawful duties, in furtherance of a valid law enforcement purpose. Sample valid law enforcement purposes include:
- i. For persons who are detained for offenses that:
 - a. Warrant arrest or citation or
 - b. Are subject to lawful identification requirements and are lacking positive identification in the field.
 - ii. For a person who an officer reasonably believes is concealing his or her true identity and has a reasonable suspicion the individual has committed a crime other than concealing his or her identity.
 - iii. For persons who lack capacity or are otherwise unable to identify themselves and who are a danger to themselves or others.
 - iv. For those who are deceased and not otherwise identified.

8.3. POLICY APPLICABILITY AND LEGAL COMPLIANCE

- (a) This policy was established to ensure that all images are lawfully obtained, including face recognition probe images obtained or received, accessed, used, disseminated, retained, and purged by the CIU. This policy also applies to:
- i. Images contained in a known identity face image repository and its related identifying information.
 - ii. The face image searching process.
 - iii. Any results from face recognition searches that may be accessed, searched, used, evaluated, retained, disseminated, and purged by the CIU.
 - iv. Lawfully obtained probe images of unknown suspects that have been added to unsolved image files, pursuant to authorized criminal investigations.
- (b) All CIU personnel, participating agency personnel, and authorized individuals working in direct support of CIU personnel (such as interns), personnel providing information technology services to the CIU, private contractors, and other authorized users will comply with DPD and the CIU's face recognition policy and will be required to complete the training referenced in section 8.11. In addition, authorized CIU personnel tasked with processing face recognition requests and submissions must also complete the specialized training referenced in section 8.11.
- (c) An outside agency, or investigators from an outside agency, may request face recognition searches to assist with investigations only if the outside agency is a law enforcement agency that is making the request based on a valid law enforcement purpose that falls within the authorized uses listed in section 8.2 and the requestor provides a case number and contact information (requestor's name, requestor's agency, address, and phone number) and acknowledges an agreement with the following statement: The result of a face recognition search is provided by DPD only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF

ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.

- (d) All technology associated with face recognition, including all related hardware and software support, is bound by the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Security Policy, particularly Policy Area 13, and the Michigan CJIS Security Addendum.
- (e) The information within the face recognition database(s) is considered highly restricted personal information and PII which may only be transmitted, accessed, used, disseminated, and disposed of in accordance with state and federal laws, rules, policies, and regulations; including, but not limited to, the most recent federal CJIS Security Policy, the Michigan CJIS Security Addendum, the CJIS Policy Council Act (1974 PA 163), MCL 28.211-28.216, and the most current CJIS Administrative Rules.
- (f) Improper access, use, or dissemination of highly restricted personal information or PII obtained from the use of the face recognition software may result in criminal penalties and/or administrative sanctions. Criminal violations include, but are not limited to, those found in MCL 28.214 and MCL 257.903.

8.4. ACQUIRING AND RECEIVING FACE RECOGNITION INFORMATION

- (a) DPD's face recognition system can access and perform face recognition searches utilizing the following entity-owned face image repositories: DataWorks Plus.
- (b) The CIU is also authorized to access and perform face recognition searches utilizing the following external repositories: Statewide Network of Agency Photos (SNAP).
- (c) In addition to above, the CIU is authorized to submit requests for face recognition searches to be performed by external entities that own and maintain face image repositories.
- (d) For the purpose of performing face recognition searches, authorized CIU personnel will obtain probe images or accept probe images from authorized requesting or participating agencies only for the authorized uses identified in 8.2.
- (e) The CIU can receive probe images from other law enforcement agencies, as long as it falls within the SNAP Acceptable Use Policy. If a non-law enforcement entity wants to submit a probe image for the purpose of a face recognition search, the entity will be required to file a criminal complaint with the appropriate law enforcement entity prior to the search.
- (f) The CIU and, if applicable, any authorized requesting or participating agencies will not violate First, Fourth, and Fourteenth Amendments and will not perform or request face recognition searches about individuals or organizations based solely on their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, gender identities, sexual orientations, or other classification protected by law.
 - i. However, DPD accords special consideration to the collection of face images relating to First Amendment-protected events, activities, and affiliations. Because of the sanctity of the First Amendment, law enforcement's role at First Amendment-protected events is usually limited to crowd control and public safety. If, however, during the planning assessment and approval process for the particular event, before proceeding with the collection, the CIU anticipates a need for the collection of face images, the member assigned to vetting the event shall submit a request to DPD's Legal Advisor on a DPD-

568 through channels. The Legal Advisor will articulate whether collection of face images through video of the event is permissible. The memo shall include the legal or justified basis for such collection (including specifics regarding the criminal behavior that is suspected); and how face images may be collected, used, or retained, in accordance with this policy, as appropriate. If face images will be collected, the plan will specify the type of information collection that is permissible, identify who will collect face images, and define the permissible acts of collection.

8.5. USE OF FACE RECOGNITION INFORMATION

- (a) Access to or disclosure of face recognition search results will be provided only to individuals within the entity or in other governmental agencies who are authorized to have access and have completed applicable training outlined in section 8.11, and only for valid law enforcement purposes (e.g., enforcement, reactive investigations), and to IT personnel charged with the responsibility for system administration and maintenance.
- (b) The CIU will prohibit access to and use of the face recognition system, including dissemination of face recognition search results, for the following purposes:
 - i. Non-law enforcement purposes (including but not limited to personal purposes).
 - ii. Any purpose that violates the U.S. Constitution or laws of the United States, including the protections of the First, Fourth, and Fourteenth Amendments.
 - iii. Prohibiting or deterring lawful individual exercise of other rights, such as freedom of association, implied by and secured by the U.S. Constitution or any other constitutionally protected right or attribute.
 - iv. Harassing and/or intimidating any individual or group.
 - v. Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.
- (c) DPD may connect the face recognition system to any interface that performs live video, including cameras, drone footage, and body-worn cameras. The face recognition system may be configured to conduct face recognition analysis on live or recorded video.
- (d) The following describes the CIU's manual and automated face recognition search procedure, which is conducted in accordance with a valid law enforcement purpose and this policy.
 - i. Authorized CIU personnel will submit a probe image of a subject of interest through the face recognition system.
 - ii. Trained CIU authorized examiners will initially run probe images without filters, using a filtered search as a secondary search, if needed. In some cases, enhancements may be considered after running an image as is against the image repository.
 - iii. Prior to executing the search, the member must enter the reason for the search within the application, as well as an associated case number, if available. Reasons may include the following:
 - a. Consent – when an individual consents to have his or her photograph taken for the purpose of identification.
 - b. Reasonable suspicion of a crime – A reasonable suspicion that an identifiable individual has committed a criminal offense or is involved in or planning criminal

- (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal conduct or activity.
- c. Physical/mental incapacity – When an individual is unable to provide reliable identification due to physical incapacitation or defect, mental incapacitation or defect, or death, and immediate identification is needed to assist DPD in performance of his or her lawful duties.
 - d. Comparison to multiple IDs – For comparison to determine whether an individual may have obtained one or more official state driver's licenses or identification cards that contain inaccurate, conflicting, or false information.
 - e. Identification of other persons of interest – To assist in the identification of potential witnesses and/or victims of violent crime.
- iv. In the automated search, most likely candidates are returned to the requestor ranked in order based on the similarity or confidence level.
 - v. The resulting candidates, if any, are then manually compared with the probe images and examined by an authorized trained examiner. Examiners shall conduct the comparison of images, biometric identifiers, and biometric information in accordance with their training.
 - a. If no likely candidates are found, the requesting entity will be informed of the negative results with the following standard response: "No likely candidates were found with the probe image given."
 - b. In the case of a negative result, the images examined by the examiner will not be provided to the requesting entity.
 - vi. Examiners will submit the search and subsequent examination results for a peer review of the probe and candidate images for verification by other authorized, trained examiners.
 - vii. All results of most likely candidate images from the face recognition search must be approved by a trained supervisor prior to dissemination.
 - viii. The CIU member shall fill out a Facial Recognition product template for all requests that return likely candidates with the following information:
 - a. The reason facial recognition search request
 - b. The requestor's name and title and date and time requested
 - c. The original probe image(s), along with any modified image and a description of the type of modifications made to the image
 - d. Source of image
 - e. Possible image matches
 - f. The face recognition software used
 - g. The following statement will accompany the released most likely candidate image(s) and any related records: "The result of a facial recognition search provided by the Detroit Police Department is only an investigative lead and is

NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.”

- ix. The CIU member shall log this in the Information Tracker SmartSheet, along with attachments of the original image plus any modified image, noted in the name.

8.6. SHARING AND DISSEMINATING FACE RECOGNITION INFORMATION

- (a) The CIU’s face recognition search information will not be:
 - i. Sold, published, exchanged, or disclosed to commercial or private entities or individuals except as required by applicable law and to the extent authorized by DPD’s agreement with the commercial vendor.
 - ii. Disclosed or published without prior notice to the originating entity that such information is subject to disclosure or publication. However, DPD and the originating agency may agree in writing in advance that DPD will disclose face recognition search information as part of its normal operations, including disclosure to an external auditor of the face recognition search information.
 - iii. Disclosed on a discretionary basis unless the originating agency has provided prior written approval or unless such disclosure is otherwise authorized by DPD and the originating agency.
 - iv. Disclosed to unauthorized individuals or for unauthorized purposes.
- (b) The CIU will not confirm the existence or nonexistence of face recognition information to any individual or agency that would not be authorized to receive the information unless otherwise required by law.

8.7. DATA QUALITY ASSURANCE

- (a) Original probe images will not be altered, changed, or modified in order to protect the integrity of the image. Any enhancements made to a probe image will be made on a copy, saved as a separate image, and documented to indicate what enhancements were made, including the date and time of change.
- (b) CIU examiners will analyze, review, and evaluate the quality and suitability of probe images, to include factors such as the angle of the face image, level of detail, illumination, size of the face image, and other factors affecting a probe image prior to performing a face recognition search.
- (c) The integrity of information depends on quality control and correction of recognized errors which is key to mitigating the potential risk of misidentification or inclusion of individuals in a possible identification. CIU will investigate, in a timely manner, alleged errors and malfunctions or deficiencies of face recognition information or, if applicable, will request that the originating agency or vendor investigate the alleged errors and malfunctions or deficiencies. The CIU will correct the information or advise the process for obtaining correction of the information.

8.8. SECURITY AND MAINTENANCE

- (a) Access to DPD face recognition information from outside the facility will be allowed only over secure networks. All results produced by the CIU as a result of a face recognition search are disseminated by secured electronic means (such as an official government e-mail address). Non-electronic disseminations will be conducted personally or by phone with the requestor or designee.

- (b) Authorized access to DPD's face recognition system will be granted only to personnel whose positions and job duties require such access and who have successfully completed a background check and the training referenced in section 8.11 Training.
- (c) Usernames and passwords to the face recognition system are not transferrable, must not be shared by CIU personnel, and must be kept confidential.
- (d) Queries made to DPD's face recognition system will be logged into the system identifying the user initiating the query. All user access, including participating agency access, and queries are subject to review and audit.

8.9. INFORMATION RETENTION AND PURGING

- (a) All members shall follow DPD's information retention policies in relation to face recognition searches and images.
- (b) In accordance with Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies, "[a]gencies should limit the retention of information as much as possible to avoid the perception of maintaining files on groups or persons who engage in protected First Amendment activities."
- (c) Images accessed by DPD for face recognition searches in SNAP are not maintained or owned by DPD and are subject to the retention policies of the respective agencies authorized to maintain those images.

8.10. ACCOUNTABILITY AND ENFORCEMENT

- (a) If CIU personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the collection, receipt, access, use, dissemination, retention, and purging, the Commanding Officer of the CIU will:
 - i. Suspend or discontinue access to information by the CIU personnel, the participating agency, or the authorized user.
 - ii. Apply appropriate disciplinary or administrative actions or sanctions.
 - iii. Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.
- (b) DPD reserves the right to establish the qualifications and number of personnel having access to DPD's face recognition system and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating this face recognition policy.

8.11. TRAINING

- (a) DPD's face recognition policy training program will cover:
 - i. Elements of the operation of the face recognition program, including:
 - a. Purpose and provisions of the face recognition policy.
 - b. Substance and intent of the provisions of this face recognition policy and any revisions thereto relating to collection, receipt, access, use, dissemination, retention, and purging of DPD's face recognition information.
 - c. Policies and procedures that mitigate the risk of profiling.

- d. How to implement the face recognition policy in the day-to-day work of the user, whether a paper or systems user.
 - e. Security awareness training.
 - f. How to identify, report, and respond to a suspected or confirmed breach.
 - g. Cultural awareness training.
- ii. Elements related to the results generated by the face recognition system, including:
 - a. Originating and participating agency responsibilities and obligations under applicable federal, state, or local law and policy.
 - b. The P/CRCL protections on the use of the technology and the information collected or received, including constitutional protections, and applicable state, local, and federal laws.
 - c. Face recognition system functions, limitations, and interpretation of results.
 - d. Mechanisms for reporting violations of CIU and DPD face recognition policy provisions.
 - e. The nature and possible penalties for face recognition policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.
- iii. In addition to the training described, CIU face recognition examiners are required to complete advanced specialized training to include:
 - a. Face recognition system functions, limitations, and interpretation of results.
 - b. Use of image enhancement and video editing software.
 - c. Appropriate procedures and how to assess image quality and suitability for face recognition searches.
 - d. Proper procedures and evaluation criteria for one-to-many and one-to-one face image comparisons.
 - e. Candidate image verification process.